Introduction to Cryptography

Alvin Lin

January 2018 - May 2018

Elliptic Curve Cryptography

Asymmetric schemes like RSA and El Gamal require exponentiations in integer rings and fields with parameters of more than 1000 bits. This requires a lot of computational effort and are difficult to store on small or embedded devices. Smaller field sizes providing equivalent security are desirable. Elliptic Curve Cryptography uses a group of points (instead of integers) for cryptographic schemes with coefficient sizes of 160-256 bits, reducing the computational effort significantly.

Abelian Group

An Abelian group is a set of elements with a binary operation, denoted by $\bullet$, that associates to each ordered pair (a, b) of elements in G an element $(a \bullet b) \in G$ such that the following axioms are obeyed.

- Closure: If a and b belong to G, then $a \bullet b$ is also in G.
- Associative: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all a, b, c in G.
- Identity Element: There is an element e in G such that $a \bullet e = e \bullet a = a$ for all a in G.
- Inverse Element: For each a in G, there is an element a^{-1} in G such that $a \bullet a^{-1} = a^{-1} \bullet a = e$.
- Commutative: $a \bullet b = b \bullet a$ for all a, b in G.

Elliptic Curves over the Reals

Elliptic curves are not ellipses. They are named so because they are described by cubic equations, similar to those used for calculating the circumference of an ellipse. In general, cubic equations for elliptic curves take the following form, known as a **Weierstrass equation**:

$$y^2 + axy + by = x^3 + cs^2 + dx + e$$

where a, b, c, d, e are real numbers and x and y take on values in the real number system. For our purpose it is sufficient to limit ourselves to equations of the form:

$$y^2 = x^3 + ax + b$$

Such equations are said to be cubic, or of degree 3, because the highest exponent they contain is a 3. Also included in the definition of an elliptic curve is a single element denoted O and called the **point at infinity** or the **zero point**. To plot such a curve, we need to compute

$$y = \sqrt{x^3 + ax + b}$$

For given values of a and b, the plot consists of positive and negative evalues of y for each value of x. Thus, each curve is symmetric about $y = 0$. The identity point O is added to the group definition. Elliptic curves are symmetric along the $x - axis$. Up to two solutions y and $-y$ exist for each quadratic residue x of the elliptic curve. For each point $P = (x, y)$, the inverse or negative point is defined as $-P = (x, -y)$.

Group elements are defined as all points (x, y) on some elliptic curve $y^2 = x^3 + ax + b$ and O, the identity point. This is an infinite group and the group operation is customarily called "point addition", symbolized using the + sign.

Computations on Elliptic Curves

Generating a group of points on elliptic curves is based on the point addition operation $P + Q = R$: $(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$.

Elliptic Curve Point Addition and Doubling

$$\begin{aligned} x_3 &= s^2 - x_1 - x_2 \mod p \\ y_3 &= s(x_1 - x_3) - y_1 \mod p \\ s &= \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \mod p & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} \mod p & \text{if } P = Q \end{cases} \end{aligned}$$

Elliptic curves can not just be defined over the real numbers $\mathbb{R}$ but also over many other types of finite fields.

Application in Cryptography

Elliptic curve cryptography uses curves whose variables and coefficients are finite. There are two families of elliptic curves used in cryptography applications:

- Binary curves of $GF(2^m)$: All variables and coefficients take on values in $GF(2^m)$ and calculations are performed over $GF(2^m)$. This is best for hardware applications.
- Prime curves over $\mathbb{Z}_p$: These use cubic equations in which the variables and coefficients all take on values in the set of integers from 0 to $p-1$ and in which calculations are perfoemd module p. This is best for software applications.

Elliptic Curves over Prime Fields

The elliptic curve $E_p(a, b)$ over $\mathbb{Z}_p, p > 3$ is the set of all pairs $(x, y) \in \mathbb{Z}_p$ which fulfill

$$y^2 = x^3 + ax + b \mod p$$

together with an imaginary point of infinity O, where $a, b \in \mathbb{Z}_p$ and the condition $4a^3 + 27b^2 \neq 0 \mod p$.

- These points form a finite group. Note that $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ is a set of integers with modulo p arithmetic. There is no obvious geometric interpretation of elliptic curve arithmetic over finite fields.
- The algebraic interpretation used for elliptic curve arithmetic carries over since point addition is the same as before, except all arithmetic is done modulo p.
- If $P = (x, y)$, the inverse $-P = (x, -y)$
- $P + (-P) = O$

Example

Given $E : y^2 = x^3 + 2x + 2 \mod 17$ and point $P = (5, 1)$, compute $2P = P + P = (5, 1) + (5, 1) = (x_3, y_3)$.

$$\begin{aligned} s &= \frac{3x_1^2 + a}{2y_1} \\ &= (2 \cdot 1)^{-1}(3 \cdot 5^2 + 2) \\ &= 2^{-1} \cdot 9 \equiv 9 \cdot 9 \equiv 13 \mod 17 \\ x_3 &= s^2 - x - 1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \mod 17 \\ y_3 &= x(x_1 - x_3) - y_1 = 13(5 - 6) - 1 = -14 \equiv 3 \mod 17 \\ 2P &= (5, 1) + (5, 1) = (6, 3) \end{aligned}$$

Example

Consider an elliptic curve $y^2 = x^3 + 5x + 7 \mod 19$. To find all the group elements, we need to find the numbers that are squares modulo 19. Then for each value of x, we ask if $z = x^3 + 5x + 7$ is a square modulo 19. If z is a square, then points $(x, \sqrt{z})$ are group elements. The point at infinity O is always a group element. The points on an elliptic curve and the point at infinity O form **cyclic subgroups**.

Number of Points on an Elliptic Curve

How many points can be on an arbitrary elliptic curve? Consider the previous example of $E : y^2 = x^3 + 2x + 2 \mod 19$. This curve has 19 points. However, determining the point count on elliptic curves in general is hard. Hasse's Theorem bounds the number of points to a restricted interval. Given an elliptic curve modulo p, the number of points on the curve is denoted by $\#E$ and is bounded by:

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$$

The number of points is close to the prime p.

Elliptic Curve Discrete Logarithm Problem

Given a primitive element P and another element Q on an elliptic curve E, the elliptic curve discrete logarithm problem is finding the integer d where $1 \leq d \leq \#E$ such that:

$$P + P + \cdots + P \ (d \text{ times}) = dP = Q$$

Cryptosystems are based on the idea that d is large and difficult for attackers to compute. Consider the group $E_2 3(9, 17)$. This is the group defined by the equation $y_2 \mod 23 = (x^3 + 9x + 17) \mod 23$. What is the discrete logarithm d of $Q = (4, 5)$ to the base $P = (16, 5)$? The brute force method is to compute multiples of P until Q is found.

$$\begin{aligned} P &= (16, 5) \\ 2P &= (20, 20) \\ 3P &= (14, 14) \\ 4P &= (19, 20) \\ 5P &= (13, 10) \\ 6P &= (7, 3) \\ 7P &= (8, 7) \\ 8P &= (12, 17) \\ 9P &= (4, 5) \end{aligned}$$

Because $9P = (4, 5) = Q$, the discrete logarithm $Q = (4, 5)$ to the base $P = (16, 5)$ is $d = 9$. In a real application, d would be so large as to make the brute force approach infeasible. If d is known, an efficient method to compute the point multiplication dP is required to create a reasonable cryptosystem. The square and multiply algorithm can be adapted to elliptic curves, but here it is known as the double and add algorithm.

Double and Add Algorithm

If P is a point (elliptic curve group element) and n is an integer, then $n \bullet P$ is n copies of P added together using point addition. In the elliptic curve $y^2 = x^3 + 5x + 7 \mod 19$, $19 \bullet (3, 12)$ is computed by repeatedly doubling using point addition:

$$\begin{aligned} 1 \bullet (3, 12) &= (3, 12) \\ 2 \bullet (3, 12) &= (3, 12) + (3, 12) = (0, 11) \\ 4 \bullet (3, 12) &= (0, 11) + (0, 11) = (7, 9) \\ 8 \bullet (3, 12) &= (7, 9) + (7, 9) = (5, 10) \\ 16 \bullet (3, 12) &= (5, 10) + (5, 10) = (6, 5) \end{aligned}$$

Then the point multiplication is computed by adding the proper multiples of $(3, 12)$:

$$\begin{aligned} 19 \bullet (3,12) &= (16+2+1) \bullet (3,12) \\ &= 16 \bullet (3,12) + 2 \bullet (3,12) + 1 \bullet (3,12) \\ &= (6,5) + (0,11) + (3,12) \\ &= (14,3) + (3,12) \\ &= (0,8) \end{aligned}$$

Point Addition Algorithm

The point addition algorithm is an algorithm that takes an prime $p > 3$, a, b for an elliptic curve $E : y^2 = x^3 + ax + b \mod p$, and points $P_0 = (x_0, y_0), P_1 = (x_1, y_1)$ on E and outputs a point $P_2 := P_0 + P_1$.

1. If $P_0 = O$, output $P_2 \leftarrow P_1$.
2. If $P_1 = O$, output $P_2 \leftarrow P_0$.
3. If $x_0 \neq x_1$, then set
$$s \leftarrow \frac{y_0 - y_1}{x_0 - x_1} \mod p$$
and go to step 7.
4. If $y_0 \neq y_1$, then output $P_2 \leftarrow O$.
5. If $y_1 = 0$, then output $P_2 \leftarrow O$.
6. Set
$$s \leftarrow \frac{3x_1^2 + a}{2y_1} \mod p$$
7. Set
$$x_2 \leftarrow s^2 - x_0 - x_1 \mod p$$
8. Set
$$y_2 \leftarrow s(x_1 - x_2) - y_1 \mod p$$
9. Output $P_2 \leftarrow (x_2, y_2)$

Elliptic Curve Parameter Generation

Elliptic curve cryptographic algorithms require the following parameters:

- A prime modulus p
- Elliptic curve coefficients a and b
- A generator (a point on the elliptic curve) $G = (x_g, y_g)$ on which point multiplication will be done. The order of G is the value n such that $n \bullet G = O$ where n should be a large prime number.

The security of the depends on the size of n. Generating suitable elliptic curve parameters is complicated, but NIST has recommended several sets of elliptic curve parameters. `Secp256k1` refers to the parameters of the ECDSA curve used in Bitcoin. The ellipic curve equation used is $y^2 = x^3 + 7$, with $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

Security Aspects

Why are parameters significantly smaller for elliptic curves (160-256 bits) than for RSA (1024-3076 bits)?

- Attacks on groups of elliptic curves are weaker than available factoring algorithms or integer discrete logarithm attacks.
- The best known attacks on elliptic curves (chosen according to cryptography criteria) are the Baby-Step Giant-Step and Pollard-Rho method.
- The complexity of these methods on average requires roughly $\sqrt{p}$ steps before the elliptic curve discrete logarithm problem can be successfully solved. An elliptic curve using a prime p with 160 bits and roughly 2^{160} points provides a security of 2^{80} steps that are required by an attacker on average. An elliptic curve using a prime p with 256 bits (roughly 2^{256} points) provides a security of 2^{128} steps on average.

Implementation

Elliptic curve computations are usually regarded as consisting of four layers:

1. Basic modular arithmetic operations, which are computationally the most expensive.

2. Group operations implementing point doubling and point addition.

3. Point multiplication operations implemented using the double and add algorithm.

4. Upper layer protocols like Elliptic Curve Diffie-Hellman and the Elliptic Curve Digital Signature Algorithm.

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech